

Last Modified: July 19, 2016

Asana is a web and mobile application designed to help teams track their work. From tasks and projects to conversations and notifications, Asana enables teams to move work from start to finish.

Before You Begin

- Acquire an administrator account to Asana premium account.
- Acquire an administrator account to RSA SecurID Access.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of the SecurID Access manual.

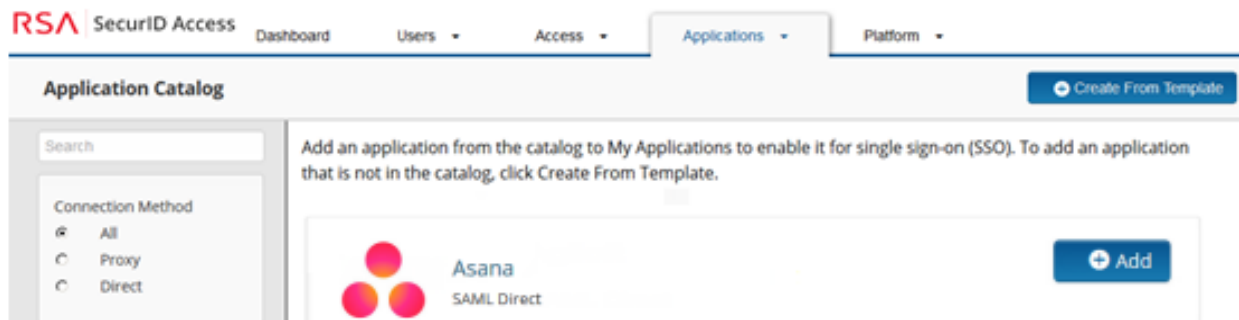
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Asana to Use RSA SecurID Access as an Identity Provider](#)

Add the Application in RSA SecurID Access

Procedure

1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, search for Asana and click **+Add**.




3. On the Basic Information page, specify the application name and click **Next Step**.

 **Note:** The following SP-initiated configuration worked for both SP and IDP connections.

4. Select **SP-initiated** and replace <yourdomain> in the Connection URL field with your Asana subdomain.
5. Select binding method **POST**.

Initiate SAML Workflow


Connection URL 

IDP-initiated SP-initiated

Binding Method for SAML Request


Redirect


POST

Signed 

 No certificate loaded


6. Scroll down to **SAML Identity Provider (Issuer)** section.

Identity Provider URL 

Issuer Entity ID 

Default (idp_id): asanatest

Override

SAML Response Signature 

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

Private Key Loaded




Certificate Loaded


Include Certificate in Outgoing Assertion

- a. Take note of the Identity Provider URL; it will be needed to configure Asana.
- b. Select **Choose File** and upload the RSA SecurID Access private key.
- c. Select **Choose File** and upload the RSA SecurID Access public certificate.

7. Scroll down to the **Service Provider** section.

Service Provider

Assertion Consumer Service (ACS) URL 

Audience (Service Provider Entity ID) 

- a. Verify the **Assertion Consumer Service (ACS) URL**; <https://app.asana.com/-/saml/consume>.
 - b. Verify the **Audience (Service Provider Entity ID)**; <https://app.asana.com>
8. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email Address** and **Property** to **mail**.
 9. Click **Next Step**.
 10. On the **User Access** page, select the desired user policy and click **Next Step**.


User Access

Select the access policy to determine which users are allowed to access the application.


Allow All Authenticated Users

Select Custom Policy 

Cancel

Next Step 

11. On the Portal Display page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**.

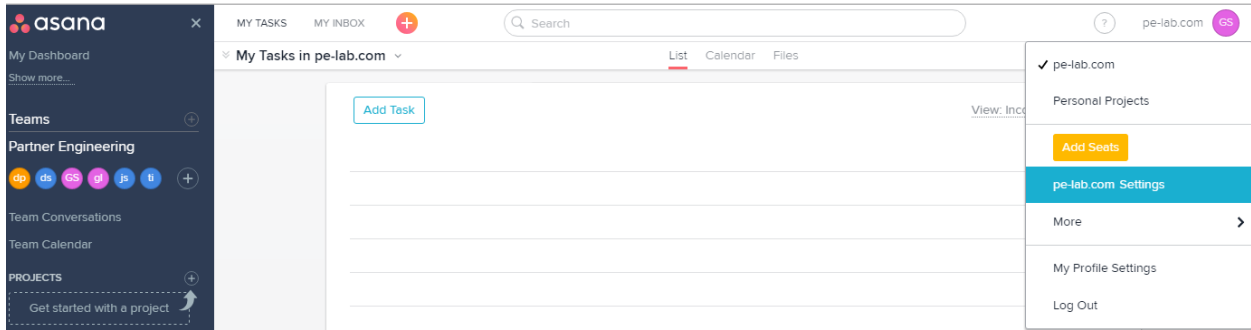
Status:  Changes Pending

Next Steps

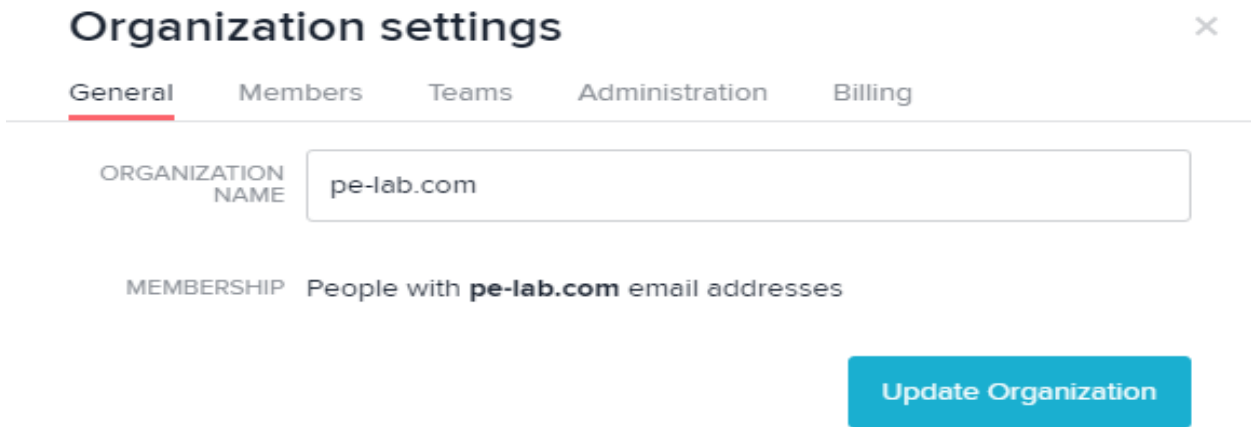
[Configure Asana to Use RSA SecurID Access as an Identity Provider](#)

Configure Asana to Use RSA SecurID Access as an Identity Provider

1. Login to your Asana Admin console.
2. Right click on your login name and select **Settings**.



3. On the Organization settings page, select **Administration**.



4. Select **Members must log in via SAML**.
5. Enter the **Identity Provider URL** from page 2 step 6 in the Sign-in page URL field.
6. Copy and paste the RSA cert.pem into the x.509 certificate field.

AUTHENTICATION

- Members may log in with an Asana Account and password
- Members must log in with their Google Account
You must log in to Google with your gsalvalzo@pe-lab.com email to turn on this feature.
- Members must log in via SAML**
SAML allows your organization to use its own system to manage the identities of its members. [Learn more >](#)

Members may also log in with email/password.
When checked, SAML is enabled but not required. Uncheck this when you've verified SAML is working.

Sign-in page URL

`https://pe108.prod0.pe-lab.com/IdPServlet?idp_id=asana`

URL for your SAML identity provider sign-in page.


X.509 Certificate

`MIIcPDCcAYygAwIBAgIGAVGMZf+XMA0GCSqGSIb3DQ`

The X.509 certificate from your SAML identity provider.

[Edit Settings](#)

7. Click **Save**.

 **Note:** To authenticate using the SP initiated flow, go to <https://app.asana.com/a/<yourdomain>> and you will be redirect to RSA for login.
